



Wege aus dem Update Dschungel

Florian Brand – ASQF 2005

Agenda

- Grundlagen
- Risiken und Nebenwirkungen
- Updates im Netzwerk
- Red Hat Network

Warum updaten?

- Mythos: Unwichtiges System
- Sicherheitsupdates zeitnah einspielen
- Bugfixes nach Bedarf
- Nicht benutzte Software nicht installieren
- **nicht ob, sondern wann.**

RPM Package Manager

- CPIO Archiv mit zusätzlichen Headern
- Abhängigkeiten
 - Requires , Prereq, Conflicts, Obsoletes
- Skripte
 - %pre, %post, %preun, %postun
- Trigger
 - Reaktion auf Veränderung anderer Pakete
 - %triggerin, %triggerun, %triggerpostun

Was passiert beim Update

1. Skript: %pre (neues Paket)
2. Installation: Neues Paket
3. Skript: %post (neues Paket)
4. Trigger: %triggerin (beliebige Pakete)
5. Trigger: %triggerun (beliebige Pakete)
6. Skript: %preun (altes Paket)
7. Deinstallation: Altes Paket
8. Skript: %postun (altes Paket)
9. Trigger: %triggerpostun (beliebige Pakete)

Problematische Pakete

■ GLIBC:

- erfordert Neustart vieler Daemons
- Reboot ratsam
- Vorsicht beim Updaten über das Netz

■ Kernel:

- Update löscht Module des alten Kernels
- Deshalb:

```
# rpm -ivh kernel-<version>.<arch>.rpm
```

Risiken bei Updates

- Veränderter Syntax der Konfiguration
- Inkompatibles API
- Datenverlust
- Ausfallzeiten bei Fehlschlag

Test der Updates

- Updates sollten zunächst auf einem identischen Testsystem aufgepielt werden.
- Anschliessender Test der Applikation(en)
- Aufwand rechnet sich nur bei unternehmenskritischen Systemen

Backports

- Bugfixes werden in der Community durch neue Versionen realisiert.
- Neue Version bedeutet (oft) neue Features.
- Neue Features gefährden die Kompatibilität.
- Besser: Rückportierung des Bugfixes auf die ursprüngliche Version.
- Hoher Aufwand, sollte daher vom Distributor übernommen werden.

Paketsignaturen

- garantieren Echtheit der Pakete
- Schutz auch bei gehacktem Updateserver
- Test mit:

```
# rpm -K <Paket Datei>  
foobar.rpm: (sha1) dsa sha1 md5 gpg OK
```
- Eigene Pakete signieren mit:

```
# rpm --resign <Paket Datei>
```
- Public Key des Distributors muss installiert sein:

```
rpm --import <PublicKey Datei>
```

Paket Verifizierung

- Vergleich des Dateisystems mit dem "Sollzustand" der RPM-Datenbank:

```
# rpm -V <Paket>
```

```
S.5...T c /etc/foobar.cfg
```

- Zeigt alle Veränderungen an.
- aber:
 - Keine Kryptographische Sicherheit
 - erkennt nur Dateien, die von RPM verwaltet werden

Grenzen von RPM

- Auflösen von Abhängigkeiten über lokale Datenbank

rpm -ivh --aid <Paket>

- Zusätzliche Pakete werden nur aus einem bestimmten Verzeichnis installiert
- Update des gesamten Systems schwierig
- Inter-Versionsupdates nur über Anaconda zuverlässig

Netzwerk Updates: apt/yum

■ apt

- einfache Bedienung
- Webserver gestützte Repositories
- keine Multi-Lib Unterstützung

■ yum

- Repositories können sowohl apt als auch yum unterstützen
- Multi-Lib Unterstützung

Netzwerk Updates: up2date

- Standard in Red Hat Enterprise Linux
- Installiert nur signierte Pakete
- Quellen
 - Red Hat Network
 - apt/yum Repositories
 - Verzeichnisse

Strategien im Rechenzentrum I

- Beseitigung von Sonderfällen
- Keine "händische Installation" auf Produktivmaschinen
- Eingenkompilate vermeiden
- Eigene Software paketieren
- Automatisierung der Installation mit Kickstart

Strategien im Rechenzentrum II

- Bereithaltung der Software & Updates auf zentralem System
- Skriptgesteuertes Einspielen der Updates
- Zentrale "Inventarisierung" der Software

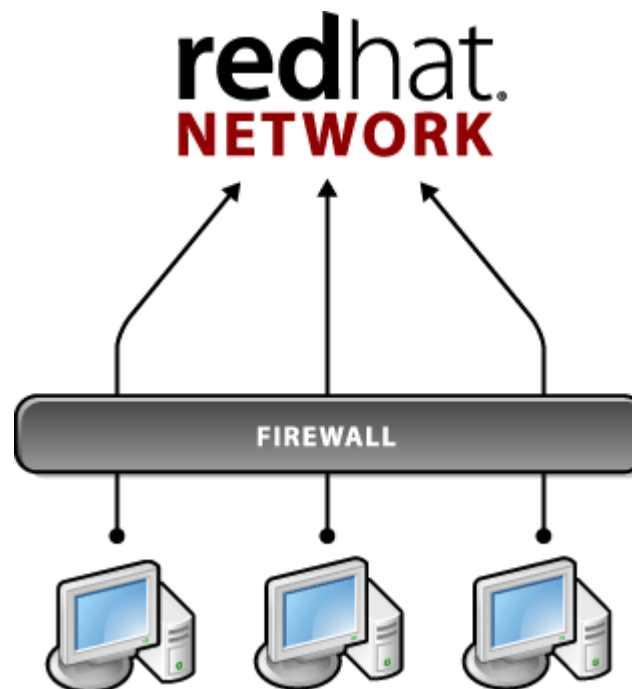
Beispiel: Red Hat Network

- Webbasierte Administration der Software Updates
- Datenbankgestützt
- Rechner können als Gruppe verwaltet werden
- Verwaltung von Config-Dateien möglich
- Kombination mit Kickstart
- Damit ist auch ein Recovery nach einem Ausfall möglich

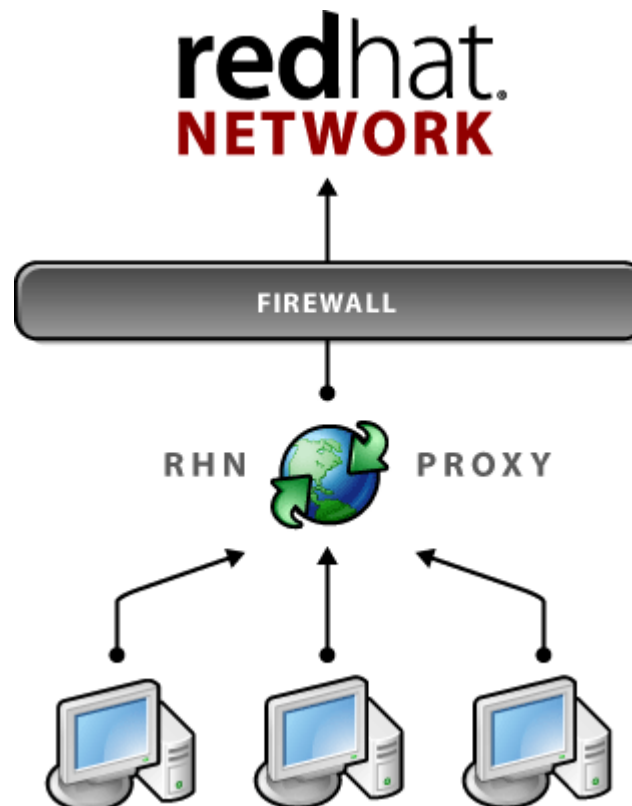
Architektur

- Verteilungsmethoden
 - Hosted (rhn.redhat.com)
 - RHN Proxy
 - RHN Satellite
- Module:
 - Update
 - Management
 - Provisioning
 - Monitoring (Preview)

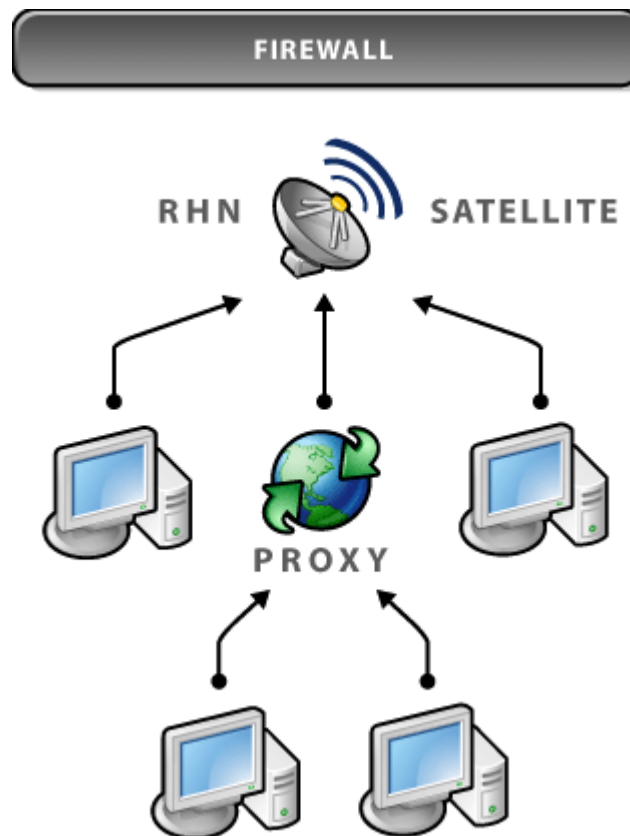
Hosted



RHN Proxy




RHN Satellite



Sicherheit

- Verbindung wird vom Client per https aufgebaut
- Zertifikat des Servers muss bereits auf dem Client installiert sein
- nur signierte Pakete werden installiert

Arbeiten mit Gruppen



redhat.NETWORK

Your RHNSystemsErrataSoftwareScheduleUsers

RHN_demo : [Sign Out](#)

Systems

Search

3 systems selectedManageClear

OverviewSystemsSystem GroupsSystem Set ManagerSystem EntitlementsAdvanced SearchActivation Keys

System Group Legend

- Fully Updated
- Critical Updates
- Updates

Buy Now

Extra EntitlementsPriority AccessEasy ISOs

System Groups

create new group

Filter by Group Name: Go

1 - 9 of 9 (0 selected)

Select	Status	Group Name	Systems	Use in SSM
<input type="checkbox"/>	!	Application Servers	1	Use Group
<input type="checkbox"/>	!	Database	3	Use Group
<input type="checkbox"/>	!	Demo Servers	3	Use Group
<input type="checkbox"/>	!	Developer Workstations	122	Use Group
<input type="checkbox"/>	✓	Laptops	0	Use Group
<input type="checkbox"/>	✓	Raleigh servers	0	Use Group
<input type="checkbox"/>	!	San Jose	49	Use Group
<input type="checkbox"/>	!	web servers	161	Use Group
<input type="checkbox"/>	!	Workstations	3	Use Group


Update ListSelect All

1 - 9 of 9 (0 selected)


Work With Intersection

Work With Union

Verwaltung eigener Software



[Your RHN](#) [Systems](#) [Errata](#) **[Software](#)** [Schedule](#) [Users](#) [Tools](#)

 [Help](#)



rhn-test-02 : [Sign Out](#)

Systems

Search

No systems selected [Manage](#) [Clear](#)

[Channels](#)
[Channel Entitlements](#)
[Advanced Search](#)
[Manage Channels](#)
[Manage Packages](#)

 **Channel: AS clone** 

[delete channel](#)

[Details](#) [Subscribers](#) [Managers](#) [Packages](#)

[Edit Channel](#)

Create or edit channels from this page.

If the parent channel is set to 'none', the channel is a base channel. Otherwise, the channel is a child of the specified channel.

Channel name and label are required. They each must be at least 6 characters in length. Labels must begin with a letter, contain only lowercase letters, hyphens ('-'), periods ('.'), numerals. Channel name may also contain spaces.

Channel summary is also required.

Parent Channel:	(none)
Channel Name:	<input type="text" value="AS clone"/> Ex: Custom Channel
Channel Label:	as-clone
Base Channel Architecture:	ia32
Globally Subscribable:	<input type="checkbox"/> Only selected users in your organization may subscribe to this channel.
Channel Package Summary:	n/a
Channel Summary:	<input type="text" value="AS clone"/>

Danke für Ihre Aufmerksamkeit!

- Slides:

<http://people.redhat.com/fbrand>

- Kontakt:

fbrand@redhat.com